In air combat, "the merge" occurs when opposing aircraft meet and pass each other. Then they usually "mix it up." In a similar spirit, Air and Space Power Journal*'s "Merge" articles present contending ideas. Readers are free to join the intellectual battlespace. Please send comments to aspj@maxwell.af.mil.*

Cyber ACTS/SAASS

A Second Year of Command and Staff College for the Future Leaders of Our Cyber Forces

Maj Paul D. Williams, USAF, PhD*

At the dawn of airpower, the Army Air Corps created the Air Corps Tactical School (ACTS), which focused upon developing tactics, techniques, and procedures (TTP) as well as doctrine that would best use airpower in war. Currently, the Air Force's School of Advanced Air and Space Studies (SAASS) at Maxwell AFB, Alabama, produces highly capable warfare strategists in support of the joint fight. We need to blend ideas from these two programs into a school that develops cyber power leaders capable of guiding the Air Force into a future where we can fly, fight, and win in air, space, and cyberspace to support America's military objectives.

The Air Force is struggling to determine the best way of developing offensive and defensive capabilities for cyber warfare. Our war-fighting prowess across the land, sea, air, and space domains relies upon our ability to maneuver freely within cyberspace. Preserving that ability represents a critical defensive requirement. We must also become capable of holding at risk our adversaries' capacity to maneuver within cyberspace. This article introduces a concept concerning how and why our service should cultivate cyber-oriented warrior-scholars who can shape the Air Force fight in cyberspace.

In many ways, cyber warfare is in its "Billy Mitchell" days, analogous to the advent of airpower prior to World War II. We are aware of potential and actual risks in this new domain but do not fully understand them. Just as ACTS gave rise to modern airpower, so do we need a school that produces cyber-oriented warrior-scholars who can help guide the future Air Force. One possibility involves adding a second year of technical study of the cyber domain to the foundation in operational art and science offered by Air Command and Staff College (ACSC) at Maxwell. Such a second-year cyber school already exists within Air University: the intermediate developmental education (IDE) cyber warfare program at the Air Force Institute of Technology (AFIT), located at Wright-Patterson AFB, Ohio.[1] I propose that the Air Force create a two-year professional military education (PME) path consisting of ACSC followed by AFIT's cyber warfare program, paralleling the current path of ACSC followed by SAASS.

The Missing Ingredient

China, North Korea, and other countries have well-developed graduate education programs in cyber warfare.[2] Additionally, these nations send students to America's finest graduate institutions for master's and doctoral degrees in cyber disciplines such as computer science, computer engineering, and electrical engineering. These stu-

*The author is an Air Command and Staff College student who previously served as a faculty member at the Air Force Institute of Technology, where he specialized in research and education related to cyber warfare.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber ACTS/SAASS: A Second Year of Command and Staff College for the Future Leaders of Our Cyber Forces	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Institute (AFRI),155 N Twining Street,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**9**	

dents return to their countries and apply their new knowledge towards developing cyber warfare capabilities. Although they may or may not use those capabilities against us, we need to consider the model they are following.

Air Force Doctrine Document 1-1, *Leadership and Force Development*, distinguishes between education and training as follows:

> Education provides critical thinking skills, encouraging exploration into unknown areas and creative problem solving. Its greatest benefit comes in unknown situations or new challenges. Thus, education prepares the individual for unpredictable scenarios. Conversely, training is focused on a structured skill set, and the results of training performance should be consistent. Thus, training provides the individual with skill expertise. Education and training together provide the tools for developing Airmen.[3]

The current Air Force and Department of Defense (DOD) methodology for developing cyber warfare forces heavily emphasizes training instead of education. The expense of training in a budget-constrained environment compels us to field forces that are trained and equipped to respond to only a limited range of scenarios. These forces find themselves out of their depth when faced with the unpredictability of a trained *and educated* adversary. This is not a winning strategy—in fact, it is not a strategy at all. As we build cyber capabilities, we need to counter the enemy's "best athletes" with our own, led by highly educated and innovative warrior-scholars.

Fundamentally, operations in a new war-fighting domain such as cyberspace take place in a fog of uncertainty and new challenges. The situation we face today resembles the one confronted by early airpower advocates during the interwar period. Specifically, a comprehensive understanding of cyber warfare does not exist; there are only a handful of outspoken proponents of cyber warfare; and most people in the Air Force and other services have little idea what cyber warfare brings to their own mission, much less the joint war-fighting environment. To many people, cyber warfare is synonymous with communications; cyber attack means corrupting Web pages; and cyber defense means keeping our Web pages safe from attack and removing viruses from our administrative networks. From this perspective, it is hard to see how cyber warfare has much to offer as a war-fighting discipline; consequently, we find little popular support for the Air Force's push into cyberspace.

The popular perception is not far off the mark. Cyber warfare capabilities in the Air Force and DOD are still nascent, and many of the ones we do have are classified to the point that the joint force commander's (JFC) staffs cannot readily incorporate them into their plans. Inside the Air Force, it is difficult to develop advocacy for undeveloped and unproven cyber capabilities, forces, and organizations, given that supporting the development of cyber capability means not supporting some other proven capability. Externally, the JFC has difficulty articulating requirements for capabilities that the services can then provide because we do not yet have much to offer the JFC in terms of a trustworthy, usable means of cyber war fighting, not to mention a plan for employing it in combat.

How do we address these problems? We start with an understanding of the effects needed by the JFC in current and near-future conflicts, as well as existing kinetic war-fighting capabilities. Many "operators" or war fighters in today's Air Force possess such knowledge, but the developing cyber warfare force and the supporting science and engineering community do not have a good understanding of it. Equally important is awareness of today's technological capabilities for cyber warfare and their potential direction in the near future—knowledge primarily possessed by a handful of scientists and engineers. A leadership-oriented education program that combines both sets of understanding and that encourages creative thinking as well as problem solving will produce highly innovative, technically competent war fighters. These officers will

lead the fight, identify needed improvements or new effects, and work with the research and development communities to produce new war-fighting competencies.

This needed innovation is not the sole responsibility of the war fighter. Rather, it requires the involvement of the research, technology development, planning, and programming communities, as well as others, together with the active participation of operators in the technology-development process and an openness to innovation. As a service, we have found ourselves in similar situations before. Perhaps the best analogies come from the dawn of airpower, when technically oriented senior leaders shaped the future Air Force through their struggles to provide solutions to war-fighting problems.

Historical Analogues

We find a similar situation in the struggles of leaders such as Lt Gen Elwood "Pete" Quesada and Gen George Kenney as they tackled the integration of airpower into the US arsenal before, during, and after World War II.[4] Virtually awash in a sea of change, both men commanded American forces at the beginnings of airpower and in the context of a world war. The manner in which these two iconic leaders dealt with our nation's war-fighting problems—specifically, their innovative exploration and adoption of technology as well as their pragmatic approach to war fighting—offers the Air Force valuable insights. Both Quesada and Kenney dealt with strategic and tactical puzzles by tossing aside dogma and searching for ways to improve the war-fighting effectiveness of their forces. These searches focused on continuous improvement, which entailed extensive experimentation followed by the adoption of workable ideas. Of particular interest is the fact that all of this innovation proceeded during the heat of battle—a notion that is anathema to the Air Force's current risk-averse culture. Both Quesada and Kenney had a complicated relationship with the prevalent service culture of their day, which emphasized strategic bombing rather than close air support and interdiction. A similar situation exists today in the Air Force's understandable preference for the air weapon over cyber or space weapons. Both leaders matured in the pre–Air Corps Army, and this background and education gave them a shared understanding of and common language with the ground commanders they supported. Correspondingly, the current airpower-oriented officers who will shape the future cyber forces share an airpower background with the air commanders they will work with and support. From a strategic perspective, as junior officers, Quesada and Kenney spent time with senior leaders, gaining broad insights into many of the important issues of the period. Upon taking command, the two generals emphasized frequent meetings with the ground commanders to enhance the situational awareness of both sides. Moreover, they spent a great deal of time in the field identifying problems, devising fixes, recognizing accomplishments of their troops, and, in general, leading from the front of efficient, energetic, and effective organizations that thrived in a wartime environment.

From a cyber perspective, we need people who likewise will lead from the front while seamlessly integrating cyber warfare into the overall fight. They will need to work closely with the leadership as well as rank and file of the organizations upon which they rely—just as Quesada and Kenney supported the ground commanders.

Information, which serves as the foundation both of modern society and of military effectiveness, remains vulnerable to cyber attack. Warfare theorists such as Martin van Creveld inform us that, throughout history, although technology has brought promise of increased war-fighting power, it is characterized by vulnerabilities and limitations. Victory in future conflicts depends upon understanding and overcoming the limitations of technology while minimizing dependence upon vulnerable technology.[5] Because we are not likely to divest ourselves of high-tech, information-dependent gad-

gets, we must determine how to fly, fight, and win in the face of determined and capable adversarial actions against those information systems. Doing so will require innovation, courage, and conviction from our leaders. The risk-taking and mission-oriented focus of Quesada and Kenney, who managed the interplay of command and technology in the context of war, offers us inspiration and motivation.

New capabilities will demand flexible leaders who can develop new TTPs and doctrine in conjunction with researchers, technology developers, and operators. Such a process calls for a mix of education (which provides broad understanding not only of theory but also of problem-solving skills), training (in a variety of weapon systems), operational experience, and a solid understanding of how the joint fight takes place. Creativity and problem-solving skills are important characteristics of the future cyber warrior, whether they be JFC planners, researchers, operators in the field, or staff officers. The cyber schoolhouses must become laboratories for conceptualizing and developing cyber war-fighting capabilities, much as ACTS was for Quesada and Kenney prior to World War II.

The Value of a Second-Year School

Air University's SAASS, the Air Force's second-year graduate school, graduates strategists and warrior-scholars who possess superior abilities to develop, evaluate, and employ airpower in conjunction with land and sea capabilities in complex war-fighting environments.[6] Its predecessor, the School of Advanced Airpower Studies (SAAS), was created in 1988 primarily to develop strategists.[7] The Air Force redesignated SAAS as SAASS in 2002.

Equivalent programs, such as the Army's School of Advanced Military Studies, the Naval Operational Planner Course, and the Marine Corps' School of Advanced Warfighting, develop advanced war fighters in their respective services.[8] The Joint Advanced Warfighting School turns out advanced campaign planners and strategists for the Joint Staff and combatant commands.[9] The three service schools build upon an operationally focused foundation of first-year graduate studies in the Air Force's Air Command and Staff College, the Army's Command and General Staff College, and the Marine Corps' Command and Staff College residence programs.

Graduates of the advanced service schools have become some of the most influential strategists and leaders in their domains, able to leverage a broad understanding of the art of war and the dynamically evolving capabilities of our military forces into effective strategies against our enemies. The success of these officers' support of the JFC in achieving operational and strategic objectives demonstrates the value of advanced war-fighting education. The model of enhancing the broad war-fighting backgrounds provided to in-residence IDE graduates with higher education in a particular area offers an effective means of grooming influential and productive leaders who possess both depth and breadth in their war-fighting domains.

Cyber Not a Good Fit for SAASS

As the Air Force determines where to add an advanced cyber curriculum to its educational system, it is logical to consider enhancing an existing program such as SAASS. Simply put, however, that school is not the right place to develop a cyber equivalent of ACTS. The Air Force originally intended SAASS as an airpower school, but its charter to produce advanced warfare strategists drives a largely service-neutral curriculum—graduates develop joint strategies realized by using the full range of war-fighting capabilities across the air, land, sea, space, and cyberspace domains.[10] SAASS students extensively examine theory and historical experience, developing an enhanced ability to think critically about how best to apply modern air, land, sea, space, and cyber-

space power across the entire spectrum of conflict.[11] The curriculum and focus remain general purpose and nontechnical.

In contrast, cyber warfare is inherently highly technical and new enough that leaders in this domain must likewise become technically proficient, much as the technical depth acquired by Quesada and Kenney contributed to their successes in terms of early airpower development. Adding an appropriate level of theoretical and engineering depth to SAASS not only would prove very expensive (e.g., hiring the appropriate faculty) but also would likely severely shortchange the strategy components of the curriculum. Ultimately, the development of cyber warfare TTPs, doctrine, and capability does not reasonably fit into a course of study concerned with domain-neutral strategy. This dilemma drives the need for a separate school.

An Earlier, Similar Proposal for Space

The Air Force space community faced a comparable situation in the 1990s, and similar ideas arose about the need for space power advocates. The service decided to include material about space in the SAASS curriculum and to keep air and space officers together in the same program.[12] The goal of having air, space, and cyber power advocates and strategists in the same room makes a great deal of sense, and of all of the Air Force's PME schools, with the exception of AFIT, SAASS has incorporated the most cyber material into its curriculum. At this point, the analogy breaks down. Instead of emphasizing general strategy, we need a program that seeks to understand the technology and theoretical underpinnings of the capabilities of cyber warfare and the way they can be leveraged alongside other joint capabilities in meeting the JFC's objectives. In this regard, the argument for a separate school reflects the need for ACTS before World War II. Current cyber strategists are trying to lift themselves up by their bootstraps, and programs such as the one leading to AFIT's cyber warfare degree can help significantly.

AFIT's IDE Cyber Warfare Program

AFIT developed the IDE cyber warfare (ICW) program, which culminates in a master of cyber warfare degree, to support the handful of IDE students sent to that school in lieu of the in-residence ACSC program.[13] The first students entered the program in 2007 and graduated in 2008. Because of its origins as an IDE program, the one-year ICW program's starting and graduation dates already match up with SAASS's.

ICW develops technical and leadership expertise in cyber warfare and cyber operations, with emphasis on the operational and strategic levels of war. The curriculum features education and research into the protection of friendly operations in cyberspace, coupled with the attack against or disruption of adversary capabilities. Ultimately, it produces proponents of cyber warfare who understand and can articulate how best to apply cyber power (offensive and defensive) in order to achieve strategic and operational military objectives. Although ICW concentrates on the cyber realm, cyber operations are closely related to information operations. Joint, Air Force, and sister-service doctrine for information operations establishes the foundation for technological constructs provided by the program. ICW's offerings encompass a wide variety of disciplines—both technical and nontechnical aspects—including the following:

- influence operations, psychological operations, and deception
- command and control warfare
- electronic warfare
- electronic sensors
- communications systems and networks
- computer and network attack, defense, and exploitation

- threat/vulnerability assessments and risk management
- legal/ethical aspects of cyber warfare
- strategic and tactical planning for cyber operations and warfare

As a war-fighting domain, cyberspace is undergoing rapid transformation, a trend that will continue for the foreseeable future. This implies that the educational development of our cyber leaders will require correspondingly rapid transformation. ICW's curriculum is developed and taught by the faculty of AFIT's Center for Cyberspace Research, which the secretary and chief of staff of the Air Force recently designated the Air Force's Cyberspace Technical Center of Excellence.[14] In this role, the Center for Cyberspace Research acts as a unifying body for promoting cyberspace education, training, research, and technology development. Its location at the juncture between the Air Force's operational cyber forces and various cyber research, education, and training communities across the service, DOD, and national organizations ensures that programs such as ICW stay on the cutting edge of technology and theory.

Selection of Students for the ICW Program

Following the model of SAASS, a centralized process should competitively select officers from a pool of volunteers. Although all graduates of first-year residence schools should be eligible, this program has the main goal of developing advocates who will lead cyber warfare forces in developing cyber capabilities in support of the JFC's objectives. Thus, selection criteria should favor officers who will likely lead cyber units, integrate cyber into the planning process, or act as cyber advocates on joint and service staffs. Accordingly, Air Force specialty code (AFSC) 33S (communications), 14N (intelligence), 11X (pilots), 13S (space and missile operations), and 12X (electronic warfare / navigator) officers and their sister-service peers would become the most likely prospects for attending such a program.[15]

How many cyber warrior-scholars do the Air Force and DOD need? SAASS graduates 40 advanced strategists and airpower advocates each year. Forty cyber graduates annually would be a terrific start. However, an initial cadre of 15 to 20 cyber-oriented warrior-scholars who can bring to the fight both the operational breadth provided by in-residence IDE and the technological depth conferred by ICW would constitute a powerful force for developing cyber capabilities in support of the joint fight. Granted, this article is Air Force centric, but the cyber fight is joint and interagency; therefore, programs such as this one should be open to all future leaders in cyberspace warfare.

Relationship to Cyber Force Development

This proposal is consistent with the Air Force mandate to develop operationally capable cyber warfare officers. Under the guidance of Headquarters Air Force/A3 and Air Force Cyber Command (Provisional), our service has spent more than two years developing a strategy to organize and train the new cyber warfare forces.[16] The development effort culminated in April 2008 with an official Air Force strategy for developing cyberspace professionals. In that strategy, the secretary and chief of staff called for development of trained, educated warriors capable of tailoring cyber effects against enemy centers of gravity and integrating them seamlessly with the full spectrum of Air Force and joint kinetic and nonkinetic effects.

Downsides of the Proposal

The Air Force has too few officers in the field already. Clearly, the prospect of having officers attend school for an additional year will not improve that situation. We must also consider costs related to management and

permanent change of station (PCS), a significant issue in today's budget-constrained environment. Although we cannot downplay such real costs, they do represent an investment in the Air Force's cyber capability that will pay substantial dividends. Fortunately, due to recent decreases in student flows, AFIT has sufficient capacity to absorb 15–20 additional ICW students, thus confining the majority of the programmatic costs to management overhead and PCS expenses.

Potential Courses of Action

If the concept of a second-year school to develop cyber-oriented warrior-scholars makes sense for the Air Force, then we have at least three possible courses of action available to us:

Establish a New Air Force Program Dedicated to Developing Cyber-Oriented Warrior-Scholars

This program would parallel the ACSC-to-SAASS program and consist of the resident ACSC program followed by the resident AFIT ICW program. Competitively chosen from the 11X, 12X, 13S, 14N, and 33S AFSC in-residence school graduates, students would go into key positions after completion of their studies.[17] The program's timelines would match those of ACSC/SAASS.

Pros. ACSC would give graduates of this program in-depth understanding of the operational art of war and employment of airpower, and AFIT's ICW would give them similar understanding of cyber warfare and the creation of cyber power. They would have both technical and operational proficiency, which would enable them to generate the innovative thought needed to develop cyber power as a war-fighting function; they would also become respected and influential leaders of the cyberspace forces. Because their selection for in-residence school has already identified them as probable senior leaders, they have a good chance of occupying key positions following the program. Finally, ACSC teaches officers how to use airpower to fight and win at the operational level of war. The cyber education from AFIT's ICW would enable advocates of cyber power to integrate both kinetic and nonkinetic capabilities across the war-fighting spectrum.

Cons. The primary downside to this course of action is cost. Moreover, officers remain out of the fight for two years in order to complete the program, which involves two PCSs—one to ACSC and another to AFIT.

Send More Officers through AFIT's ICW

Selected from the 11X, 12X, 13S, 14N, and 33S IDE in-residence list, students would go to AFIT along the lines of the current IDE program and hold key cyber and related positions after program completion.

Pros. No significant programmatic or management changes need occur. This option also incurs only one IDE-related PCS, and students would be out of the fight for only one year.

Cons. Primarily, graduates would not receive the in-depth education in operational art and the science of war offered by the in-residence ACSC program, whose lectures and seminar discussions add substantially to a student's understanding of the material. This deficiency may decrease graduates' ability to integrate cyber power with air and space power.[18]

Re-create the AFIT ICW Program at Maxwell, Perhaps inside SAASS

This program, which parallels the ACSC-to-SAASS program, consists of the resident ACSC program followed by the Maxwell ICW program. Competitively chosen from the 11X, 12X, 13S, 14N, and 33S AFSC in-residence school graduates, students hold key cyber and related positions after program completion.[19] Timelines match those of ACSC/SAASS.

Pros. The same as the ones for the first course of action.

Cons. The principal downsides involve the difficulty and expense of duplicating the educational capability in technical engi-

neering and science that exists at AFIT, whose ICW program requires classified and unclassified laboratory and classroom space, classified and unclassified network connectivity, and extensive technical equipment. The most significant difficulty would entail creating and maintaining an appropriate, effective graduate-level engineering faculty, usually requiring many years to develop. Finally, one of the main advantages of AFIT's ICW curriculum is that the faculty members are part of the Air Force Center for Cyberspace Research, which allows them to stay on the leading edge of cyber warfare through teaching, research, and outreach—an association not available to faculty at Maxwell. Finally, officers in the program would remain out of the fight for two years.

Recommendation and Conclusion

I recommend the first course of action—establishing a new Air Force program dedicated to developing cyber-oriented warrior-scholars. Though expensive in terms of time and the cost of an additional PCS, it offers the best education to officers who attend. The second course of action, increasing the number of students in the current AFIT ICW program, would face the disadvantages discussed above but might serve well as an initial step while the programmatics of the first course of action are developed. The third option, duplicating the ability to teach an ICW-like program at Maxwell, is the least viable choice, primarily due to the duplication of capabilities as well as the high cost.

This program may not need to be permanent—the Air Force's abilities to fly, fight, and win in cyberspace will likely solidify into mainstream processes in 10 to 15 years. Until then, we need to determine how graduates of ACTS and SAAS were able to make the most of the new airpower capabilities. Following this model will enable the Air Force to develop cyber power fully and to integrate it seamlessly into our war-fighting capabilities. AFIT's ICW program, already up and running, can accommodate 15–20 additional students each year. I recommend that the Air Force follow the ACTS/SAAS/SAASS path by creating a second-year graduate path that emphasizes cyber and that parallels SAASS. Just as all second-year PME graduates have proven influential in raising American war-fighting power to its current heights, so will ICW graduates become innovative, forward-thinking officers able to guide our Air Force towards a future in which we can counter all potential adversaries in air, space, and cyberspace. ✪

Maxwell AFB, Alabama

Notes

1. "ICW IDE Cyber Warfare Program Guide," http://www.afit.edu/en/eng/PDF/Program%20Guide%20-%20Cyber%20Warfare2.pdf (accessed 3 October 2008).

2. Timothy L. Thomas, *Dragon Bytes: Chinese Information-War Theory and Practice from 1995–2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004), 18–23; and Senator Mary Landrieu, "Combating Threats from Cyberspace," *Hill*, 17 June 2008, http://thehill.com/op-eds/combating-threats-from-cyberspace-2008-06-17.html (accessed 15 November 2008).

3. Air Force Doctrine Document 1-1, *Leadership and Force Development*, 18 February 2006, 26, http://www.dtic.mil/doctrine/jel/service_pubs/afdd1_1.pdf.

4. See Thomas Alexander Hughes, *Over Lord: General Pete Quesada and the Triumph of Tactical Air Power in World War II* (New York: Free Press, 1995); and Thomas E. Griffith Jr. *MacArthur's Airman* (Lawrence, KS: University of Kansas Press, 1998).

5. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 261–75.

6. School of Advanced Air and Space Studies, Air University, http://www.au.af.mil/au/saass/ (accessed 3 October 2008).

7. Stephen D. Chiabotti, "A Deeper Shade of Blue: The School of Advanced Air and Space Studies," *Joint Force Quarterly* 49, 2nd quarter (April 2008), http://www.ndu.edu/inss/Press/jfq_pages/i49.htm (accessed 27 April 2009).

8. See Command and General Staff College, United States Army Combined Arms Center, http://usacac.army.mil/CAC2/cgsc/; Naval Operational Planner Course, http://www.nwc.navy.mil/academics/courses/nop.aspx (accessed 17 May 2009); and School of Advanced Warfighting, Marine Corps University, http://www.tecom.usmc.mil/mcu/csc/saw/index.htm (accessed 6 January 2009).

9. See Joint Advanced Warfighting School, National Defense University, http://www.jfsc.ndu.edu/schools_programs/jaws/overview.asp (accessed 6 January 2009).

10. School of Advanced Air and Space Studies (see note 6).

11. Col G. Scott Gorman, commandant, School of Advanced Air and Space Studies, interview by the author, 7 January 2009.

12. Lt Col Bertrand Sparrow, DEI deputy chair, Air Command and Staff College, Maxwell AFB, AL, to the author, e-mail, 14 October 2008.

13. "ICW IDE Cyber Warfare Program Guide."

14. Center for Cyberspace Research, Air Force Institute of Technology, http://www.afit.edu/ccr/ (accessed 7 October 2008).

15. In 2009 or 2010, the 33S (communications and information officer) and some 12X (navigator and electronic warfare officer) AFSCs are converting to 17D (for nonrated officers) and 12W (for rated officers) cyber warfare officers, respectively. For the purposes of this article, 33S and 12X are interchangeable with 17D and 12W.

16. For an early description of that effort, see Maj Timothy P. Franz et al., "Defining Information Operations Forces: What Do We Need?" *Air and Space Power Journal* 21, no. 2 (Summer 2007): 53–63.

17. Other AFSCs, such as the 61/62/63 family of scientists and engineers, would undoubtedly benefit from this program as well. However, because they probably would not lead cyber forces, we should emphasize AFSCs most likely to capitalize on their cyber skills in the war-fighting domains.

18. At the time of this writing, the author is nearing the end of the in-residence ACSC program; he completed the nonresident program in 2007.

19. Ibid.